REGLAMENTO DE SEGURIDAD INFORMATICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE RUMIÑAHUI (GADMUR)

GESTION DE SEGURIDAD INFORMATICA

DIRECCIÓN DE TECNOLOGÌA DE LA INFORMACIÓN Y COMUNICACIÓN
VERSION 1.0
SANGOLQUI 20 DE JULIO DEL 2020

DTIC's
Montufar 251 y Espejo
2 998 300 ext. 4005
www.ruminahui.gob.ec

CONTENIDO **REGLAMENTO DE SEGURIDAD INFORMATICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE RUMIÑAHUI (GADMUR)**

OBJETIVO El presente reglamento tiene como finalidad establecer los principios criterios y requerimientos de seguridad informática que garantice la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información

RESPONSABLES De su implantación: Dirección de tecnologías de la Información y comunicaciones.
De su cumplimiento: Todo el personal del GADMUR
De su control: Dirección de tecnologías de la Información y comunicaciones.
De su actualización: Dirección de tecnologías de la Información y comunicaciones.
De su distribución y difusión: Dirección de tecnologías de la Información y comunicaciones.

I. INTRODUCCION

La base para que las organizaciones puedan operar de una forma confiable en material de seguridad informática, comienza con la definición de normas, el caso de nuestra entidad, se definen con la siguiente:

- Seguridad de Recursos Humanos
- Seguridad Lógica
- Seguridad Física
- Seguridad Legal

Seguridad de Recursos Humanos

Se establecen los principios de seguridad de la tecnología de la información que permite asegurar que los empleados, contratistas y terceros, entiendan sus responsabilidades y sean idóneos para los roles que ejecuten, de tal forma se reduzcan el riesgo del robo, fraude y mal uso de los medios informáticos

Seguridad lógica

Establece e integra los mecanismos que permiten otorgar, controlar y monitorear el acceso a los programas y archivos de los sistemas de información automatizados

Seguridad física

En este nivel se identifican los límites mínimos que se deben cumplir respecto al control físico de los recursos tecnológicos, su acceso y la transferencia de información

Seguridad legal

Integra los requerimientos que deben cumplir los servidores municipales en relación a la normativa interna y externa en materia de seguridad informática.

II. BASE LEGAL

El presente reglamento de Seguridad Informática está fundamentado en las normas de Control Interno emitidas por la Contraloría General del Estado. (Publicadas en el suplemento del registro Oficial No. 87 del 14 Diciembre del 2009, Acuerdo No. 039-CG), como referencia, se han considerado los dominios y objetivos de control de la norma internacional ISO/IEC 27002:2005.

III. AMBITO DE APLICACION

Es responsabilidad de todo usuario que tenga asignado un recurso tecnológico y que se encuentre en el ejercicio de sus funciones, ya sea personal interno o externo del GADMUR, acatar lo indicado en el presente reglamento.

IV. CONTROL DE REGLAMENTO

El reglamento de Seguridad Informática ha tomado como referencia los objetivos de control de la Norma ISO/IEC 27002:2005; consecuentemente, las direcciones de informática y de desarrollo Institucional verificaran de manera oportuna y suficiente el cumplimiento de los mencionados controles, en el ámbito de sus competencias.

V. ALCANCE

Establecer normas de seguridad de recursos de recursos humanos, lógicos, físicos y legales para precautelar la integridad de los equipos de computación de la institución o de aquellos recibidos en comodato, así como garantizar la preservación de la información del GADMUR.
Dotar de información a los usuarios del GADMUR, respecto a las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software, así como la información que se almacenada y procesada en estos.

CONCEJO MUNICIPAL DE GOBIERNO AUTONOMO DE RUMINAHUI GADMUR
CONSIDERADRO

QUE, el artículo 238 de la Constitución de la República del Ecuador declara que, los gobiernos autónomos descentralizados gozaran de autonomía política, administrativa y financiera;

QUE, el artículo 425 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, prescribe que es obligación de los gobiernos autónomos descentralizados velar por la conservación de los bienes de propiedad de cada gobierno y por su más provechosas aplicación a los objetos a que están destinados; y.

QUE, con la finalidad establecer los principios, criterios y requerimientos de seguridad informática que garantice la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información, las Direcciones de Desarrollo Institucional y de Informática Municipal han elaborado un proyecto de reglamentación respecto de la seguridad informática.

EL REGLAMENTO DE SEGURIDAD INFORMATICA DEL GOBIERNO AUTONOMO DESCENTRALIAZADO MUNICIPAL DEL GADMUR.

CAPITULO I
SEGURIDAD DE RECURSOS HUMANOS

1.1 DE LA SEGURIDAD INFORMATICA RELACIONADA AL PERSONAL

Art.1 Los servicios de la red municipal de datos son de uso exclusivo para los usuarios del GADMUR y de usuarios externos previamente autorizados por la autoridad competente.

Art.2 Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir con lo establecido en el reglamento de seguridad informática del GADMUR.

Art.3 Se entregara al contratado toda la información necesaria para ejercer sus labores dentro de la institución, durante la vigencia de su contrato laboral.

Art.4 La información procesada, intercambiada, reproducida, almacenada y conservada en los computadores de la entidad, será considerada como municipal.

Art.5 Se consideran faltas graves el robo, daño, alteración de información de los sistemas automatizados de la entidad, el uso de los sistemas para ejecutar actos como

piratería informática, penetración a otras redes, etc; o que el usuario sea judicialmente declarado culpable de un delito informático.

Art.6 Cualquier acto negligente o ataque informático hacia los activos de información (redes, sitios, sistemas internos o externos) que cause o daños a la información, será considerado como una falta grave y sancionado según lo establecido en la Ordenanza Reglamentaria del Talento Humano del GADMUR

1.2 RESPONSABILIDADES SOBRE ACTIVOS INFORMATICOS

Art.7. Todo equipo informático tendrá un custodio o responsable que velara por su cuidado y buen uso, debiendo responder en forma pecuniaria y directa en caso de cualquier pérdida o destrucción injustificada, de acuerdo con el **Manual Especifico para la administración y control de Bienes de larga duración** que para efecto emita la municipalidad.

Art.8. Los administradores de sistemas (correo electrónico, intranet, internet, sistemas transaccionales y web, bases de datos y demás sistemas futuros), designados por la Dirección de Informática, serán los responsables de la seguridad de la información en el campo de sus competencias

1.3 DE LA CAPACITACION DE USUARIOS

Art.9. Todo funcionario, servidor o trabajador que ingrese a formar parte del GADMUR, deberá recibir una inducción sobre el Manual de Políticas y Estándares de Seguridad Informática para Usuarios, donde se dan a conocer las obligaciones para los usuarios y las sanciones en caso de incumpliendo. Esta labor será realizada de manera coordinada entré las direcciones de: Recursos Humanos (Departamento de Capacitación), informática (Departamento de Seguridad Informática) y desarrollo INSTITUCIONAL (Departamento de Procesos Informáticos)

Art.10. Antes de realizar una capacitación al personal interno y externo de la institución, se tomaran las medidas de seguridad necesarias, tanto a nivel físico como lógico, la capacitación se llevara a cabo en equipos y programas del ambiente de pruebas.

1.4 DE LAS RESPUESTAS A INCIDENTES Y ANOMALIAS DE SEGURIDAD INFORMATICA

Art.11. Las solicitudes de asistencia por parte de uno o as empleados, con problemas en las estaciones de trabajo, serán atendidas a través de la Mesa de Ayuda, de acuerdo a la disponibilidad de recursos o a las prioridades establecidas para el efecto.

Art.12. Cualquier situación anómala y contraria a la seguridad de la información deberá ser tratada y documentada por un equipo de respuestas a incidentes con el objetivo de analizarla y dar una solución acorde al problema, ya sea esta en el ámbito técnico, legal o administrativo. Este equipo será designado por el director de informática o la persona que el delegue para tal efecto.

SEGURIDAD LOGICA

2.1 DE LAS POLITICAS Y ESTANDARES DE CONTROLES DE ACCESO LOGICO

Art.13. Cualquier petición de información o servicios informáticos, provenientes de un determinado usuario o departamento, se deberá efectuar siguiendo los canales de gestión y niveles de autorización formalmente establecidos en la institución.

Art.14. las direcciones de informática y de Desarrollo Institucional mantendrán en la intranet la documentación relacionada a reglamentos, normas, guías, políticas y controles de Seguridad de Información, a la que tendrá acceso todo el personal del GADMUR.

2.2 DE LA CLASIFICACION DE LA INFORMACION

Art.15. Las direcciones municipales deben considerar la clasificación de su información electrónica, de acuerdo a la importancia para la entidad y el cumplimiento de los requerimientos legales, a fin de establecer los parámetros para su acceso.

2.3 DE LA ADMINISTRACION DE ACCESO DE USUARIOS

Art.16. Son usuarios de la red municipal de datos todos aquellos usuarios que se concedido los permisos correspondientes, siguiendo el procedimiento de solicitud de Acceso al Sistema.

Art.17. Los usuarios tendrán acceso a sitios de la intranet una vez que se encuentren autenticados en la red municipal de datos y, de acuerdo a las funciones que desempeñen, se asignaran sus permisos correspondientes.

Art.18. Para el acceso a opciones consideradas como “restringidas” la Dirección de informática solicitara que exista una autorización de la dirección propietaria de los datos, previo a otorgar el permiso correspondiente.

Art.19. Se considera usuario externo a cualquier persona natural o jurídica que tenga una relación con la institución fuera de ámbito de empleado, siempre que tenga una vinculación con los servicios de la red municipal de datos.

Art.20. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible solo mediante firma empresa de un acuerdo de confidencialidad hacia la institución, con el compromiso del uso exclusive del servicio para el que fue provisto. Este tipo de acceso será autorizado por el director de Informática o su delegado

Art.21. La contraseña de usuario de la red municipal de datos se establece siguiendo el procedimiento previsto en el Manual de Políticas de la Dirección de Tecnologías de la información y Comunicación.

2.4 DE LAS RESPONSABILIDADES DEL USUARIO

Art.22. El usuario será responsable exclusive de mantener a salvo la privacidad de su contraseña.

Art.23. El usuario será responsable del buen uso de su cuenta de acceso a los sistemas o servicios.

Art.24. Es obligación del usuario cambiar la clave por defecto asignada por la Dirección de Tecnologías de la Información y Comunicaciones.

Art.25. Se debe evitar guardar o escribir las contraseñas en cualquier papel o superficie, o dejar constancia de ellas.

Art.26. Las claves son individuales; está prohibido que los usuarios la compartan o releven a terceros, siendo de su exclusive responsabilidad el uso de la misma.

Art.27. Cuando a un usuario se le olvide, bloquee o caduque su contraseña, deberá solicitar a la Dirección de Tecnologías de la Información y Comunicaciones el restablecimiento respectivo. Esta acción será realizada por el responsable de seguridad Informática tomando las medidas suficientes para evitar la suplantación de la identidad del empleado.

Art.28. El usuario deberá definir contraseñas seguras, siguiendo los parámetros previstos en el Manual de Políticas de la Dirección de Tecnologías de la Información y Comunicaciones.

Art.29. Cuando Tengan que alejarse de sus estaciones de trabajo, los usuarios deberán bloquear, a través del sistema operativo, los equipos de computación a fin de proteger la información de acceso no autorizados.

Art.30. Cualquier usuario que encuentre una vulnerabilidad en la seguridad de los sistemas informáticos del GADMUR, sea porque la computadora que usa no tiene instaladas todas las actualizaciones del software de base o su antivirus esta desinstalado o deshabilitado, está obligado a reportado al responsable de seguridad informática.

Art.31. El respaldo de la información que los usuarios mantengan en sus equipos de computación será de su exclusiva responsabilidad. La Dirección de Tecnologías de la Información y Comunicaciones no se responsabilizara por la pérdida voluntaria o involuntaria de información en equipos.

Art.32. Sera responsabilidad del responsable Seguridad Informática deshabilitar del servicio de directorio de la red distribuida de computadores del GADMUR, las cuentas de los usuarios de los ex empleados municipales. En los casos de renuncia, se mantendrá un acceso limitado únicamente a las opciones que su jefe inmediato autorice durante el tiempo que la ley establece para la entrega definitiva de su cargo.

Art.33. Cuando exista la sospecha o el conocimiento de que alguna información haya sido revelada, alterada o borrada, sin la autorización respectiva, el usuario deberá notificar a la Dirección de Tecnologías de la Información y Comunicaciones, que a su vez emprenderá el análisis correspondiente para determinar el origen, usuario y circunstancia de la actividad.

2.5 DEL USO DEL CORREO ELECTRONICO INSTITUCIONAL

Art.34. El correo electrónico es de uso exclusivo para los usuarios del GADMUR es personal e intransferible. A cada usuario se le creara su propia cuenta y está prohibido utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo.

Art.35. El Usuario será responsable de la información que sea enviada a través de su cuenta de correo eléctrico.

Art.36. La Dirección de Tecnologías de la Información y Comunicaciones, podrá acceder y analizar los mensajes y archivos adjuntos enviados a través del correo institucional, al existir sospecha o denuncia de envió de información que comprometa la seguridad de la red, o cualquier otra acción no autorizada.

Art.37. Tanto los mensajes enviados y recibidos, así como los archivos adjuntos que salen y entran a los buzones institucionales, se consideran propiedad del GADMUR.

Art.38. El usuario debe utilizar el correo electrónico exclusivamente para asuntos relacionados a las funciones que el fueron asignadas a su cargo, empleo o comisión, se Prohíbe utilizar el correo electrónico con fines personales para distribuir o reproducir información no relacionada a la institución.

Art.39. Queda prohibido suplantar, falsear o alterar la identidad de un usuario de correo electrónico.

Art.40. Queda prohibido el interceptar, ayudar a interceptar o revelar a terceros, las comunicaciones por correo electrónico.

Art.41. Se prohíbe utilizar en el correo institucional lenguaje inapropiado y/o palabras ofensivas que afecten la honra y estima de terceros.

Art.42. Para él envió de información reservada y/o confidencial, vía correo electrónico, se deberá utilizar la firma electrónica, y debe estar destinado exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

2.6 DE LA SEGURIDAD DE ACCESO A TERCEROS.

Art.43. Todo usuario externo estará facultado a utilizar única y exclusivamente el servicio informático que le fue asignado, y asumir las responsabilidades de su uso.
Art.44. Los accesos a la red interna, por parte de terceros, contemplarán los mismos controles de acceso utilizados para los usuarios internos, además de los requisitos expuestos a sus contratos con el GADMUR.

2.7 DEL CONTROL DE ACCESO A LA RED

Art.45. El acceso a la red interna será exclusive a equipos de computación del GADMUR; en caso de dispositivos particulares, se podrán conectar a la red excepcionalmente, siempre y cuando se justifique su propósito laboral y cumplan con los requisitos de seguridad y autentificación.

Art.46. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos será motive de verificación y tendrá como resultado directo la realización de una auditoria a la red municipal de datos.

Art.47. Se registrara todo acceso a los dispositivos de red, mediante archivos de registro o archivos log de sistemas.

Art.48. Sera considerado como un ataque informático y alta grave, cuando un usuario, con fines de detector y explotar una posible vulnerabilidad, realice la exploración de los recursos informáticos o aplicaciones de la red municipal de datos.

Art.49. El director de informática autorizara las restricciones de tiempo para las sesiones de trabajo de los usuarios, mientras que el responsable de seguridad informática le corresponderá verificar que el sistema lleve los registros de uso. Las restricciones de tiempo deben revisarse ante cualquier cambio del estado laboral del usuario, con ascenso, remoción o terminación de contrato.

Art.50. El director de informática autorizara el acceso a la red inalámbrica interna dependiendo de las características de seguridad del dispositivo con el que se desea conectar el usuario.

2.8 DEL CONTROL DE ACCESO AL SISTEMA OPERATIVO

Art.51. Los funcionarios del GADMUR deberán tener en cuenta que la identificación del usuario y la contraseña, que les fueron asignados por la Dirección de Tecnologías de la Información y Comunicaciones, son para el acceso al sistema operativo del computador y a otros servicios de información (tales como e-Mas y SharePoint); por lo cual, tomaran las medidas de seguridad necesarias a fin de evitar acceso no autorizados por terceros.

2.9 DE LOS EQUIPOS SERVIDORES

Art.52. El acceso a la configuración del sistema operativo de los equipos servidores, es únicamente permitido a los administradores de sistemas designados por la Dirección de Tecnologías de la Información y Comunicaciones.

Art.53. Los administradores de sistemas tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tiene bajo su responsabilidad**.**

2.10 DEL CONTROL DE ACCESO A LAS APLICACIONES

Art.54. La Dirección de Tecnologías de la Información y Comunicaciones deberá definir y/o estructura el nivel de permisos sobre las aplicaciones, de acuerdo a la ejecución o gravedad de las aplicaciones o archivos y haciendo especial énfasis en los derechos de escritura, lectura modificación, ejecución o borrador de información. Para permitir el ingreso a los sistemas, la dirección solicitante deberá definir previamente los perfiles de acceso, de acuerdo a las funciones y jerarquías de los usuarios, así como rangos limitados de actividades (menús restringidos).

Art.55. La Dirección de Tecnologías de la Información y Comunicaciones deberá habilitar un equipo de prueba en el que realizara el control de calidad de cada programa, con el objetivo de evitar que en los sistemas de producción existan errores de fondo y forma.

Art.56. Se deberán llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a acceso, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde se conecta entre otros, de manera que proporcionen información relevante y revisable posteriormente.

Art.57. Se prohíbe la instalación de software que no cuente con la licencia de uso; la responsabilidad que se origine en estos casos recaerá en el usuario que la realizo.

Art.58. Los usuarios que requieran utilizar un software que no sea propiedad del GADMUR, deberán solicitarlo a la Dirección de Tecnologías de la Información y Comunicaciones, justificando su uso e indicando el equipo de cómputo donde se instalara y el periodo de tiempo que permanecerán dicha instalación.

Art.59. Se considera una falta grave que los usuarios instalen cualquier tipo de programa (software), que no esté autorizado por la Dirección de Tecnologías de la Información y Comunicaciones, en las computadoras a su cargo o cualquier equipo conectado a la red municipal de datos.

Art.60. La Dirección de Tecnologías de la Información y Comunicaciones será responsable de proveer las especificaciones técnicas ante la solicitud de adquisición o desarrollo de aplicaciones automatizadas que se requiera en la entidad, así como de evidenciar que las instalación del sistema nuevo no afecte adversamente la seguridad general ni los sistemas existentes.

Art.61. Todo sistema de información desarrollado a adquirido por el GADMUR, contara con programas, aplicaciones y procedimientos documentos, controles de acceso y seguridades, así como una segregación de funciones según el área y cargo competente, para salvaguardar la confidencialidad, integridad y disponibilidad de los datos.

2.11 DEL MONITOREO DE ACCESO Y USO DEL SISTEMA.

Art.62. Se registrara y archivara toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de log o bitácoras de sistemas.

Art.63. Los registros de log almacenaran nombres de usuarios, nivel de privilegios, IP de terminar, fecha y hora de acceso a utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros, a fin de conocer las acciones que realizan los usuarios.

2.12. DE LA GESTION DE OPERACIONES Y COMUNICACIONES

2.12.2 DE LAS RESPOSABILIDADES Y PROCEDIMIENTOS

Art.64. Las configuraciones y puesta en marcha de servicios de tecnología de información, son normadas por La Dirección de Tecnologías de la Información y Comunicaciones.

Art.65. La Dirección de Tecnologías de la Información y Comunicaciones es la responsable de mantener en óptimo funcionamiento los servicios informáticos del GADMUR.

2.12.2 DE LA PLANIFICACION Y ACEPTACION DE SISTEMAS.

Art.66. La Dirección de Tecnologías de la Información establecerá una metodología para los procesos de planificación, desarrollo, adquisición, implementación y/o adaptación de los sistemas automatizados necesarios para el GADMUR.

Art.67. La Dirección de Tecnologías de la Información y Comunicaciones es la responsable de actualizar las versiones de software, previo al análisis de los requisitos técnicos necesarios.

Art.68. Cuando una de las direcciones del GADMUR requieran un programa (software) especifico (Autocat, Ms Project, etc.), deberá solicitar a la Dirección de Tecnologías de la Información y Comunicaciones un informe técnico a fin que analice la factibilidad y parámetros de compatibilidad y seguridad acordes con los estándares técnicos municipales.

Art.69. La Dirección de Tecnologías de la Información y Comunicaciones a través de su departamento de producción investigara programas (software) alternativos que pudieran beneficiar a la buena gestión de la institución en lo que se refiere a sistemas operativos, beses de datos, lenguajes de programación y otros propios de su ámbito de acción. Si otras direcciones requieren una aplicación automatizada para agilitar su trabajo, deberán solicitar asistencia a la Dirección de Desarrollo Institucional para

definir y documentar los procesos de manera que la Dirección de Tecnologías de la Información y Comunicaciones, pueda programar o contratar el desarrollo respectivo.

Art.70. La aceptación y uso de los sistemas no impiden que el responsable de Seguridad Informática realice pruebas y controles sobre los sistemas a implementarse.

Art.71. El software desarrollado en la entidad debe cumplir con las normas internas de seguridad, por lo que antes de su implementación será revisado por el responsable de seguridad informática.

Art.72. Para la puesta en producción de un nuevo sistema, se deberá contar con la aprobación formal del área solicitante.

Art.73. Ningún usuario podrá realizar pruebas sobre sistemas en producción; por tanto, el testeo de aceptación por el área solicitante se lo realizar en el ambiente de control de calidad.

Art.74. Las solicitudes de modificación a los programas de un sistema automatizado que no signifique desarrollo de nuevos sistemas o subsistemas pero que impliquen cambios en el proceso, serán previamente evaluados por la Dirección de Desarrollo Institucional; posteriormente la Dirección de Tecnologías de la Información y Comunicaciones, será el responsable de la capacitación a los usuarios respecto a las modificaciones aplicadas en los sistemas.

2.12.3 DE LA PROTECCION CONTRA SOFTWARE MALICIOSO

Art.75. Se adquirirá y utilizara software únicamente de Fuentes reconocidas como confiables o referidas por sitios especializados en la evolución de programas automatizados.

Art.76. La Dirección de Tecnologías de la Información y Comunicaciones, deberá contar un equipo servidor dedicado exclusivamente para la gestión del software antivirus y sus funciones de actualización y protección de computadores en tiempo real.

Art.77. Es responsabilidad de cada usuario revisar, a través de software antivirus todos los medios ópticos como discos compactos, discos de almacenamiento de datos, memorias USB, para verificar que no tengan programas maliciosos, antes de usar esos dispositivos en su computadora.

Art.78. La Dirección de Tecnologías de la Información y Comunicaciones, será responsable de la instalación configuración y actualización regular los programas y sus últimas bases de datos, para la detección o reparación de códigos maliciosos.

Art.79. La Dirección de Tecnologías de la Información y Comunicaciones, configurara las herramientas de protección contra virus y códigos maliciosos, a fin de que los archivos adjuntos a los correos sean analizados previo a su descarga.

Art.80. El usuario genere, compile, escriba copie o propague programas o aplicaciones en cualquier tipo de código o lenguaje de computadora, que estén diseñados para auto-replicarse, dañar o borrar datos o impedir el funcionamiento de aplicaciones y programas autorizados o componentes del equipo computacional como memorias o periféricos, serán sancionado como una falta grave de acuerdo a lo previsto en la ordenanza reglamentaria del Talento Humano del GADMUR.

Art.81. Cualquier usuario que sospeche la infección de su equipo computacional con virus, troyano o cualquier otro código malicioso, no debe intentar erradicando por si mismo, deberá dejar de usarlo inmediatamente y comunicar del particular a la Dirección de Tecnologías de la Información y Comunicaciones, a través de la mesa de ayuda, para que se tomen las acciones respectivas de restablecimiento del equipo y eliminación del código malicioso.

Art.82. Los usuarios a quienes se les asignado equipos portátiles que no se conectan a la red municipal de datos, están en el deber de solicitar periódicamente a la Dirección de Tecnologías de la Información y Comunicaciones, la actualización del código antivirus.

Art.83. Queda prohibido a los usuarios modificar o eliminar la configuración de las consolas de antivirus instaladas en los equipos de computación.

Art.84. Ningún usuario, empleado o personal externo podrá bajar o descargar software de sistemas, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Dirección de Tecnologías de la Información y Comunicaciones.

2.12.4 DEL MANTENIMIENTO DE SOFTWARE

Art.85. El mantenimiento de las aplicaciones y actualizaciones de software de sistemas es de exclusiva responsabilidad del personal de la Dirección de Tecnologías de la Información y Comunicaciones.

Art.86. Se llevara un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

2.12.5 DEL MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

Art.87. Es responsabilidad de los usuarios almacenar su información únicamente en la parte de disco duro identificada como "D: Mis Documentos" ya que las otras están destinadas para archivos de programa y sistema operativo.

Art.88. Si un área desea bloquear los puertos de entrada (USB), solicitara a la Dirección de Tecnologías de la Información y Comunicaciones, que se implemente tales restricciones.

2.13 DEL SITIO WEB MUNICIPAL Y USO DEL INTERNET

Art.89. La Dirección de Tecnologías de la Información y Comunicaciones, será responsable de la disponibilidad continua de los sitios web del GADMUR.

Art.90. Los usuarios tendrán acceso a internet, siempre y cuando cuenten con la autorización del director del área en la que laboran, se cumplan con los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la Dirección de Tecnologías de la Información y Comunicaciones.
Los usuarios con acceso a internet se sujetaran a las normas y políticas internas previstas en el documento de "Políticas de Uso de Internet del GADMUR"

Art.91. El acceso a internet provisto a los usuarios del GADMUR es exclusivamente para las actividades relacionadas con el puesto o función que desempeña y no para propósitos personales.

Art.92. Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provisto por el GADMUR, en caso de necesitar una conexión a internet especialmente, esta tiene que ser notificada y aprobada por la Dirección de Tecnologías de la Información y Comunicaciones.

Art.93. Los usuarios con acceso a internet serán sujetos al monitoreo de las actividades que realizan.

Art.94. En lo relacionado al acceso a paginas web, los usuarios deberán acatar lo previsto en el Reglamento para la utilización del Servicio de Internet en el GADMUR Cap. V de las Restricciones.

2.14 DE LAS FIRMAS ELECTRONICAS

Art.95. Para las comunicaciones formales internas y externas se debe considerar el uso de la firma electrónica o firma digital.

Art.96. La Dirección de Tecnologías de la Información y Comunicaciones debe tener actualizado el servicio de firmas electrónicas internas.

Art.97. La Dirección de Tecnologías de la Información y Comunicaciones, debe instalar la firma electrónica en cada computador con acceso al correo electrónico interno.

Art.98. En los casos de las firmas electrónicas otorgadas por la entidad u organismo, el usuario titular es responsable del uso y actualización.

Art.99. Se debe hacer uso de la firma electrónica, según lo previsto en la ley de comercio electrónico, firmas electrónicas y mensajes de datos ecuatoriano (Titulo II Capítulo I), para garantizar la legitimidad de la información del GADMUR.

Art.100. La firma electrónica tendrá igual validez y se le reconocerán los mismo efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicios.

CAPITULO III
SEGURIDAD FISICA

3.1 DEL RESGUARDO Y PROTECCION DE LA INFORMACION

Art.101. Sera responsabilidad la Dirección de Tecnologías de la Información y Comunicaciones verificar que las áreas de trabajo cuenten con la adecuada instalación eléctrica.

Art.102. La Dirección de Tecnologías de la Información y Comunicaciones, será responsable de analizar las áreas que requieran de una fuente de alimentación ininterrumpida (UPS), debido a la naturaleza de su información y los riesgos de perdida de la misma, como por ejemplo cortes de energía.

Art.103. La Dirección de Tecnologías de la Información y Comunicaciones, será responsable de analizar las áreas donde sea necesario la instalación de un regulador de voltaje para proteger máquinas de avanzada tecnología y alto costo, con la finalidad de que las mismas no sufran daños, no cuenten con ninguna información.

Art.104. La Dirección de Tecnologías de la Información y Comunicaciones, a través de su departamento técnico, verificara que los medios de almacenamiento que contengan los equipos a dar de baja, no cuenten con ninguna información.

3.2 DE LOS CONTROLES DE ACCESO FISICO

Art.105. Los equipos o activos críticos de información y procesamiento de datos deberán ubicarse en espacios aislados y seguros, protegidos.
Art.106. El espacio donde se ubican los equipos servidores deben tener un acceso restringido, contar con una puerta blindada, un sistema biométrico para su ingreso y un control de circuito cerrado de cámaras.

3.3 DE LA SEGURIDAD EN AREAS DE TRABAJO

Art.107. El acceso durante la noche, fines de semana o feriados, hacia las áreas de procesamiento de información de la Dirección de Tecnologías de la Información y Comunicaciones debe estar debidamente justificado. El guardia de seguridad debe verificar si el usuario cuenta con la debida autorización y en el horario señalado.

Art.108. Los centros de cómputo son áreas restringidas, por la que solo el personal autorizado por el director de la Dirección de Tecnologías de la Información y Comunicaciones, pueden acceder a ellos.

3.4 DE LA PROTECCION Y UBICACIÓN DE LOS EQUIPOS INFORMATICOS

Art.109. Una vez instalados los equipos informáticos por personal autorizado, los usuarios no deben moverlos o reubicarlos, instalar o desinstalar dispositivos, ni retirar sus sellos de seguridad.

Art.110. Mientras se utilizan los equipos informáticos, no se deberán consumir alimentos p ingerir líquidos.

Art.111. No se debe colocar objetos encima de los equipos informáticos o cubrir sus orificios de ventilación.

Art.112. Se deben mantener los equipos informáticos en un entorno limpio y sin humedad.

Art.113. El usuario debe asegurarse que los cables de red no se encuentren presionados con objetos encima o contra ellos; en caso de que esta situación no se cumpla, debe solicitar la redistribución de los cables de red del departamento de soporte técnico.

Art.114. Cada usuario es responsable de los equipos informáticos, partes piezas y accesorios, desde el momento en que el departamento de control de bienes realiza la asignación correspondiente.
Art.115. El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración o custodia, aun cuando no contengan información reservada/confidencial.

Art.116. El suministro de energía eléctrica para los computadores deben hacerse a través de un circuito exclusivo, que debe contar con tomacorrientes a 120v polarizados (FASE-NEUTRO-TIERRA) y de tierra aislada. Para distinguir los tomacorrientes de los de servicio general, deben ser de color naranja y estar etiquetados con la nomenclatura "PC"; en ellos no deberán conectarse impresoras, cafeteras, microondas, aspiradoras ni cualquier dispositivo electrónico o aparato eléctrico, ya que estos equipos exceden la capacidad real del UPS, por lo que pueden provocar que este se apaguen y con el tiempo se dañe.

Art.117. La Dirección Administrativa conjuntamente con el departamento de seguridad industrial, de la Dirección de recursos Humanos, Verificara que las instalaciones eléctricas y de comunicaciones donde deban conectarse los equipos de cómputo cumplan las condiciones óptimas de seguridad (Uso de canales, identificación con marcadores de cables y equipos), se forma que se prevenga el riesgo de incendios o accidentes de trabajo.

Art.118. El cableado de la red municipal se instalara físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica para evitar interferencias.

Art.119. El Departamento de Seguridad Industrial identificara las áreas críticas para definir la ubicación y determinar el mantenimiento de detectores de humo y calor, alarmas y extintores adecuados, que serán usados en la protección de las estaciones de trabajo y equipos especiales en casos de emergencia, lo que permitirá asegurar que los referidos dispositivos se encuentre en condiciones óptimas de funcionamiento.

Art.120. La Dirección Administrativa, en todo lugar donde se encuentra instalado un equipo informativo, deberá climatizarlo a fin de evitar el calentamiento de los mismos o daños por la humedad. Aquellos equipos que se encuentren disponibles al acceso de ciudadano, deberán tener características para esos ambientes. Es aconsejable que el equipo se utilice y almacene a una temperatura de 21 , 1º C y una humedad relativa 50% , 5%

3.5 DEL MANTENIMIENTO DE EQUIPOS INFORMATICOS

Art.121. Únicamente el personal autorizado por la Dirección de Tecnología de la Información y Comunicación podrá llevar a cabo los servicios de mantenimiento y reparación a los equipos informáticos.

Art.122. La Dirección de Informática deberá ejecutar controles tanto para el mantenimiento preventivo como para el correctivo de los equipos informáticos.

Art.123. Corresponde a la Dirección de Tecnología de la Información y Comunicación a través del área de soporte técnico, planificar ejecutar y documentar el mantenimiento de los equipos informáticos.

3.6 DE LA PERDIDA O DAÑO DE LOS EQUIPOS INFORMATICOS

Art.124. El usuario que tenga bajo su resguardo algún equipo de cómputo o accesorio, será responsable de su uso y custodia; en caso de desaparición, robo o extravió, deberá dar aviso inmediato al área del Control de Bienes de la Dirección Financiera, de acuerdo con el Manual Especifico para la Administración y Control de Bienes de Larga Duración que para el efecto emita la Municipalidad.

Art.125. En caso que los equipos de cómputo o recursos de tecnología de información sufran algún daño por maltrato, descuido o negligencia por parte de su custodio, se aplicara lo previsto en el artículo 3 del Reglamento General Sustitutivo para el Manejo y Administración de Bienes del Sector Público.

3.7 DE LAS ACTIVIDADES PROHIBITIVAS

Art.126. Se prohíbe a los usuarios utilizar los equipos informáticos provistos por el GADMUR, para un objetivo distinto del que están destinadas para beneficiar a personas ajenas a la institución.

Art.127. Queda terminantemente prohibido colocar stickers o cualquier otro material adhesivo a los recursos tecnológicos que son propiedad del GADMUR.

CAPITULO IV
SEGURIDAD LEGAL

4.1 DEL LICENAMIENTO DE SOFTWARE

Art.128. Todo software que se utilice en los equipos informáticos del GADMUR y que no sea propiedad municipal, deberá contar con la respectiva licencia de uso. Únicamente se utilizara software certificado o, en su defecto, software previamente revisado y aprobado por el personal calificado en esta materia, desinado por la Dirección de Tecnología de la Información y Comunicación.

Art.129. Los sistemas desarrollados para el GADMUR, por personal interno o externo, son de propiedad intelectual de la entidad municipal: por lo tanto, no podrán reproducirse sin el permiso de su autoridad máxima, respetando la ley de Derecho de Autor y Propiedad Intelectual.

4.2 DE LOS CONTRATOS CON TERCEROS

Art.130. Los contratos con terceros, en la gestión o prestación de un servicio, deberán especificar acuerdos de confidencialidad, medidas necesarias de seguridad, nivel de prestación de servicio, además del personal involucrado en tales procesos.

4.3 DE LAS VIOLACIONES DE SEGURIDAD INFORMATICA

Art.131. Ningún usuario del GADMUR debe probar o intentar probar vulnerabilidades en la seguridad de los sistemas, a menos que estas pruebas sean aprobadas y controladas por la Dirección de Tecnología de la Información y Comunicación.

Art.132. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñados para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del GADMUR.

CAPITULO V
CONSIDERACIONES GENERALES

DE LA VIGENCIA Y ACTUALIZACION

El presente Reglamento de Seguridad Informática entrara en vigencia desde la aprobación de la máxima autoridad de la entidad.

Este reglamento deberá ser revisado y actualizado conforme a las exigencias del GADMUR, o en el momento que existan cambios sustanciales en la infraestructura tecnológica de la red municipal

CAPITULO VI
TERMINOS Y DEFINICIONES

Archivos Log: Es un registro de los eventos que ejecuta un sistema informático durante un rango de tiempo; sus datos permiten obtener quien, que, cuando, donde y por qué ocurre una acción en una aplicación automatizada.

Ataque Informático: Es un método por el cual uno o varios individuos, mediante un sistema informático, intentan tomar el control, desestabilizar o dañar otro sistema o aplicación informática.

Confidencialidad: Es garantizar que la información es accesible solo para aquellos autorizados a tener acceso.

Cuenta: Es la identificación que se otorga a un usuario y que, asociado a una contraseña, sirve para autenticarse e ingresar a un sistema informático.

Disponibilidad: Es la característica o condición de que la información pueda ser accedida cuando sea requerida por las personas, procesos o aplicaciones de la entidad.

Firma Electrónica: Es un mecanismo que permite al receptor de un mensaje firmado electrónicamente (o digitalmente), determinar le entidad de origen del mensaje y confirmar que no ha sido alterado desde que fue firmado por el originador.

GADMUR: Gobierno Autónomo Descentralizado Municipal de Rumiñahui.

Integridad: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Seguridad de la Información: Son los mecanismos utilizados para la preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, inclusive con los datos contenidos, a través de normas, procedimientos, métodos, técnicas, estándares, protocolos, regla y herramientas relacionadas a la tecnología de la información.

Servicio: En el contexto del presente reglamento, es el conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor del GADMUR
Riesgo: Es la probabilidad que una amenaza determinada afecte a un activo que procese a maneje información.

Terceros: Personas que proveen o realizan trabajos relacionados a la tecnología de la información y deben acceder a las instalaciones informáticas.

Usuario: Define al servidor municipal que utiliza los servicios informáticos de la red del GADMUR y tiene una vinculación laboral con la institución.

Vulnerabilidad: Son puntos débiles del software que permiten que un atacante comprometa la confidencialidad, integridad y disponibilidad de la información.

DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN